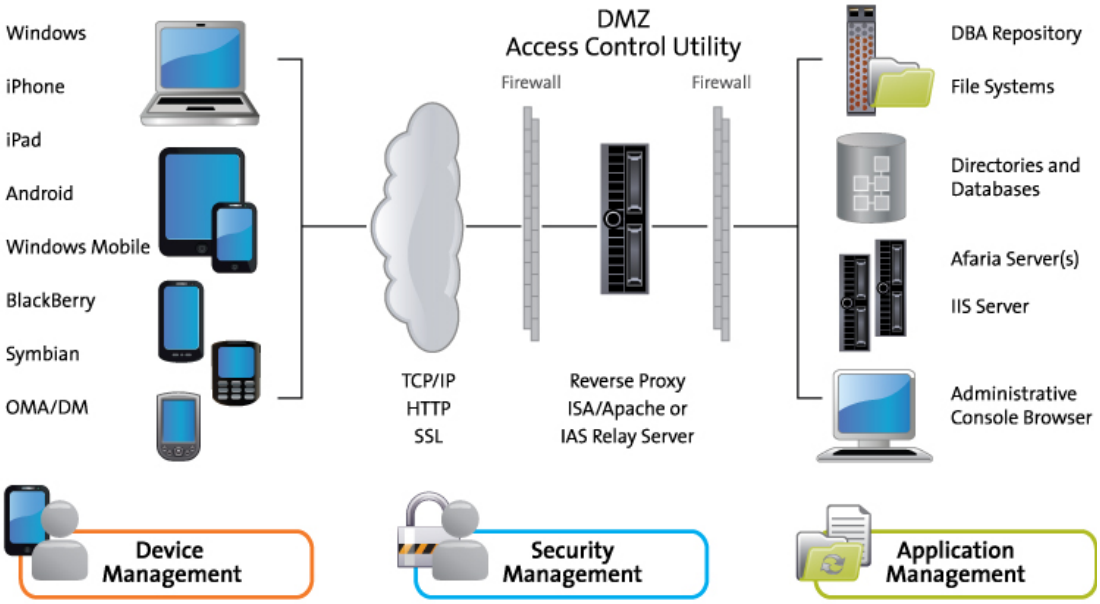
SYBASE®
An SAP Company

WHITE PAPER

Afaria: A Technical Overview

With so many mobile operating systems and device choices available, you need a solution that can manage and secure all your critical enterprise data, applications and devices. Afaria simplifies the management complexities of an on-the-go workforce by ensuring that all data stored and transmitted by mobile devices is secure. Afaria provides comprehensive device management, security and application management for all mobile devices in both a hosted and on-premise model. The diagram below depicts the basic architecture of an on-premise Afaria implementation.



CONFIGURE MOBILE DEVICES

Afaria ensures that mobile devices are configured properly and lets you securely and centrally define and maintain system attributes, preferences and settings for remote devices. Whether you are deploying personally-owned or corporate owned devices, you can rely on Afaria to take care of configuration and set up of devices. Afaria can manage ActiveSync settings, including connection settings and synchronization options. You can remotely configure connection settings, such as details about the network service, server addresses and logon information. Synchronization options for email, calendar and contact information can be configured centrally and enforced on client devices.

MANAGE MOBILE APPLICATIONS

- Deliver in-house or publically available apps to any mobile device
- Deliver applications and updates without interrupting users
- Optimize delivery methods and times
- Detect unauthorized changes and reduce exposure to unlicensed software and harmful viruses

When it comes to mobility, improving productivity by enabling access to applications and data makes all the difference. Keeping everyone's software up-to-date and working is mandatory. Afaria makes it easy for administrators to centrally distribute, install, maintain and support mobile applications, no matter what kind of device they're using, or whether the app is an in-house app or publically available on an application store like Apple's App Store or Google Marketplace.

The latest applications benefit users, but the many software distribution tasks associated with keeping those applications up-to-date can be a burden to employees. Afaria works behind the scenes to keep systems running without interfering with user's tasks and data.

Relying on remote users to remember to update applications can create havoc across the entire network. Afaria's ability to install applications, supply missing or corrupted files, and uninstall or roll back applications means that all your employees will have the correct versions, the latest updates, and the right settings at all times.

Afaria reduces the complexity of managing devices for mobile workers and IT. It also increases your knowledge of how your investments are being utilized. All of this helps you accomplish the goal you had for your implementation in the first place: productive workers empowered to do their jobs.

ENSURE ENTERPRISE SECURITY

- Enforce power-on password
- Encrypt data on device
- Enforce security policies such as remote lock and remote wipe

Mobile users face an extremely vulnerable computing environment where security gaps can exist. Smartphones, tablets and laptops can easily be lost or stolen, the risk of intrusion is high, and security controls are inconsistent at best. Additionally, government and industry regulations regarding data privacy and encryption are strict, and can even result in fines for noncompliance. It is imperative that organizations manage and protect sensitive information, and enforce security centrally, rather than leaving the burden of security to the mobile device end user.

Afaria offers unique security functionality. It enables IT to manage security requirements centrally, including enforcing power-on password, encryption of data, updating signature files and antivirus engines, and managing the configuration of the device. IT is able to increase the efficiency of managing any mobile deployment while ensuring security policies are enforced and devices remain updated.

Password protection is the first step toward securing data on mobile devices. Afaria offers IT the ability to centrally define, control and enforce end user password requirements. Power-on password capability requires a user to enter a password each time the device is cycled on, device "lock down" after a predefined number of failed password entry attempts, device reset, encrypted data deletion or complete device disablement may be enforced by IT after failed password entry attempts. Alphanumeric and/or character based passwords may be used, variable frequency of password change requirements set, and remote password retrieval by IT is possible in the case of a forgotten password.

Afaria gives users and IT high performance peace of mind by offering the ability to encrypt data that resides on devices. In the case of a lost or stolen device, data is protected through strong encryption, rendering the device unusable. In addition, IT can select what data to encrypt and when it should be encrypted. Removable storage medium, such as compact flash cards and SD cards, can also be encrypted.

Key to any corporate security effort is the ability to log and report all security activity and being able to pull and deliver detailed reports for any exceptions, violation of company security policy and devices entering and leaving service. You can generate reports by device type, groups or user type, password entry failure and redeployment of new policy upon reconnection, and you can obtain status of client delivered to handheld devices.

On some platforms, a concept referred to as data fading is possible. Afaria allows an IT administrator to lock, wipe or reset a device that has not communicated with the corporate network or Afaria server after a configurable time period. This automatically renders a device unusable, eliminating manual IT intervention for lost or stolen devices. When a device is lost or stolen, the risk of data loss increases is untenable. Fines may be imposed and a company's reputation can be irreparably damaged, so IT needs the ability to ensure data does not land in the wrong hands. Using Afaria you can send a "kill device" command to completely disable a device. Other options include hard reset of device, or deletion of data on external storage media.

Mobile threats have escalated from simply a lost or stolen device scenario to more sophisticated, invisible attacks designed to either cause irreparable harm to your mobile device or intercept sensitive company data. Afaria provides full protection from the latest mobile threats, via automatic virus definition updates, real-time monitor scans any file received via SMS, MMS, Bluetooth, WiFi, infrared, or desktop sync, inbound and outbound traffic monitoring, and blacklist and whitelist filtering of mobile spam and unwanted calls.

MANAGE DEVICES USING A SESSION-BASED APPROACH

A wide range of real-time processes can be automated through these events, including:

- Automate data retrieval from, or data delivery to, mobile devices
- Sync worker-specific content and data between the frontline device and headquarters (with or without end user involvement)
- Connect frontline solutions to backend legacy applications and data
- Automate electronic file distribution
- Automate pre- and post-software distribution processes
- Enhance application self-healing
- Enforce processes and policies, such as anti-virus policies
- Take condition-based actions, such as locking down or deleting data from devices identified as lost or stolen

The systems your mobile employees rely on are often intermittently connected to your corporate network. This kind of computing paradigm necessitates a different type of systems management approach, a session-oriented approach. Afaria uses this session-oriented approach, allowing you to automate business processes and increase communication efficiency for intermittently connected devices and systems. A flexible, scalable management software solution for companies of every size, Afaria efficiently and centrally manages the complex tasks associated with enterprise-wide distributed systems management.

Using Afaria, you can automate electronic file distribution, file and directory management, notifications, and system registry management tasks without having to learn a programming language. It provides efficient file transfers, fault-tolerant communications, incremental updates, and checkpoint restart for your desktop, laptop, and handheld devices.

Afaria is organized using a transmitter/channel paradigm. Channels consist of worklists and sendlists: organized, reusable groups of events that correspond to specific tasks which are scripted to occur when the client connects to the transmitter (server).

Afaria offers an easy-to-use graphical scripting tool that's designed for system administrators, not programmers. All of your Afaria channels, worklists, and sendlists are displayed in a tree structure so you can visually organize your channels and their components. The scripting tool can automate communication sessions; organize file and directory management tasks, such as file push and pull; change file attributes; automate processes using conditional business logic; detect connection speed; update registries; and generate alerts and messages.

Afaria gives you visibility to session activity and file transfer activity. It lets you create custom systems management tasks and specify when a given worklist, sendlist, or event is available for execution. You can fine-tune worklists and sendlists, decreasing session completion time by preprocessing tasks that can be performed on the client device before a session begins.

Afaria provides optimal device and application availability, performance and reliability to your employees, no matter where their work takes them or what devices they're using. By doing so, it lowers the cost of system maintenance while freeing your employees to focus on strategically important tasks, not the technology they use to support those tasks.

BACK UP CRITICAL CORPORATE DATA

- Archive data, applications and hardware configurations to a centralized location
- Back up information on a scheduled basis without user involvement
- Efficiently retrieve data using techniques that minimize connection times
- Remotely download lost data, applications and settings to replacement devices

The information gathered and used by mobile workers is an important corporate asset. Ensuring that this data is backed up and rapidly recoverable is both a high priority and a challenge. A centralized and automated process is the way to ensure that important information is always available. Afaria makes the data archiving and recovery process simple for individual users and effective for the larger organization. It backs up workers' critical business data and documents, ensuring their availability to both the employee and the company, even if the device is lost, damaged or stolen. Archived data, applications and hardware configurations can be quickly restored to any system or device that has been lost or damaged.

Afaria allows IT to centrally manage data backup in the background, with no user intervention. Bandwidth controls make it feasible to back up large amounts of data even over low bandwidth connections, because they reduce the volume of data sent, the bandwidth demands, and the connection time. If a backup is interrupted during a data transmission, it can be picked up where it left off during the next communication session. This avoids redundant data transmission, reducing connection time as well as user frustration.

Afaria gives you multiple ways to manage the backup and restore process. You can change the default location for backups, for example, and set space-usage thresholds that activate alerts when usage at the backup location exceeds a specified percentage. When available disk space is consumed, message log entries and alerts are generated. You can also set a specified number of days after which all backed up items will be deleted. You can restore files selectively or in full.

Back up and restore critical data from specified files, folders, and applications to a managed folder structure on the corporate network. For handheld client devices, applications and data missed by PIM sync processes are backed up and can be restored when these devices connect to the server.

CONTROL ENTERPRISE ASSETS

- Capture asset information
- Full visibility into application use
- Maintain accurate inventory
- Monitor device status

When you first deploy your mobile devices, you know how many you have, where they are located, and which applications have been installed. As time goes by, some of those devices may not be where they are supposed to be, and some aren't being used at all. It's difficult to know the exact status of all those devices, all the time. Afaria makes this task manageable by allowing you to scan and capture detailed hardware and software asset information from systems and devices like laptops, smartphones and tablets.

Afaria gives you the functionality needed to maintain accurate inventory records, monitor device status, update applications with targeted deployments, provide fast assistance to workers with hardware or software problems, find and lock down lost devices, and guarantee that corporate security policies and procedures aren't compromised when devices are lost or stolen.

The proliferation of technology—especially devices supporting mobile workers—has made it difficult to track individual copies of software residing on desktops, laptops, and handhelds. Beyond knowing what's actually installed, it's almost impossible to gauge which installed packages are actually being used, especially when employees are remote from the oversight of the IT department. How can you tell if employees really need and use the software they've been given? How can you tell if they have loaded unlicensed software onto your systems? These are important questions, given the cost of applications and the risk associated with license violations.

Afaria provides answers by giving you full visibility into application use on the device. It tracks software installation and usage data on PCs, laptops, smartphones, and tablets. This information is delivered to standard relational databases, allowing you to compare software usage against software purchases and license agreements, based on installed count, expiration date or both. The database layout is published, allowing you to access this information directly and produce custom reports that incorporate additional information such as User Department or Billing Area.

Afaria generates detailed data views, reports and alerts on license compliance providing accurate information and the ability take rapid action to resolve the problem of unlicensed software use. The cost of critical applications is high; these programs are valuable corporate assets. Afaria lets you integrate software license information—such as whether the license is a site license, a network license, a per-user/per seat license, etc.—with other enterprise systems that track and manage corporate assets.

Afaria allows you to gather accurate and complete user data so that you can truly see where applications are installed but unused. It retrieves software usage data from client devices automatically and transparently and thus makes a physical audit unnecessary. By identifying unused licenses, you open opportunities for reclaiming licenses and lowering or containing license fees. You won't get stuck with the bill for unnecessary licenses, and you can use this data to negotiate refunds or future concessions from vendors. At the very least, you can reduce or eliminate support and upgrade costs for packages no longer in use. The payoff? Hard dollar savings.

Your workers rely on software every day; you rely on them to use it appropriately. With Afaria you won't have to guess what applications are installed, what applications are being used, and whether or not you are at risk of license violation.

REMOTE CONTROL MOBILE DEVICES

- Real time remote control capabilities

Afaria offers real-time remote control capability for Windows® based PCs and handheld devices. Afaria offers the option to interactively train end users on new applications or troubleshoot specific devices. Users can connect to their devices via wired or wireless networks. All communications between the administrator console and mobile devices are secured using powerful AES encryption. Administrators can also select from a variety of configuration options that will optimize sessions for best efficiency and security in their network environment. With Afaria, mobile users always have ready access to both training and resolution of critical issues to help them remain productive.

Afaria consists of two main modules for remote control; the console and the client. The console is installed on the Windows-based computers in your organization's technical support or training department that need to access frontline computers. The client is installed on all of the Windows-based mobile computers and Windows Mobile handhelds you wish to control.

An optional third component, the Afaria Remote Control Gateway Server can be used as a point of LAN entry/exit traffic. Typically, the Gateway is used as a router to access Clients on a LAN through one port or to convert between protocols. The advantage of the Gateway is that it increases security and flexibility as it minimizes open ports in the firewall. The Gateway typically sits in the DMZ and routes traffic to computers running the Remote Control Console behind the firewall.

PATCH MANAGEMENT

- Guarantee patch delivery

With hackers increasing their efforts to exploit vulnerabilities, software patching and updating has become a major management headache. How do you distribute a large patch without interfering with mission-critical network traffic such as credit card authorization? How do you ensure a patch is fully delivered to a laptop or other device in the field that is only intermittently connected to the network?

Afaria is optimized for operations in a WAN limited bandwidth environment, and is a sophisticated patch management system that can rapidly close security exposures for increased availability of business systems. Its ability to operate over a Wide Area Network means you can send patches to remote and intermittently connected devices without negatively affecting other applications running on your network. And its scalability means you can patch hundreds, even thousands, of systems without missing a beat.

Such a system allows you to manage the utilization of bandwidth to your remote sites, so critical business processes such as credit card authorization aren't compromised, gain visibility into and do a baseline assessment of system vulnerabilities, deploy and verify deployment of patches to close those vulnerabilities, and automate the process of determining which patches are available from Microsoft, and then retrieving the necessary patches from the Microsoft Web site.

With a manual solution, an enterprise never has an accurate view of the vulnerability of its systems, so the correct patch may not be deployed. In addition, companies have little or no visibility into whether or not the patches were successfully applied to all the intended systems. As a result, security holes may be missed entirely, leaving the enterprise vulnerable to attack.

MAINTAIN CONTROL OF DOCUMENTS

- Deliver and update files
- Easily replace old documents

Working outside of an office often means that it's harder to get the latest versions of anything coming from headquarters. Pricing lists, proposal templates, promotion materials, competitive information, presentations—there's always a question of whether or not everyone's got the right version. Maybe your company's current approach is to periodically send a CD into the field, or to use email alerts to let mobile workers know that new documents are available for download. Either way, the process is cumbersome for everyone involved.

Afaria ensures that mobile workers always have the content they need. Afaria provides organized initial delivery and ongoing updates for content and data files to mobile devices, without the involvement of users. With Afaria, you can deliver and update files containing dynamic information, including text files, graphic files, and HTML files. Content can be disseminated to all users, or to selected sub-groups, as needed.

Document owners maintain control over their content and can easily replace old documents with the latest versions, allowing files to be refreshed automatically when outdated. Administrators can quickly and efficiently "push" content to users and/or allow users to subscribe to or "pull" specific files.

Afaria lets you create document management channels using server-based files and/or external media sources such as CDs. You can create different channels that all use the same media as the source, or specify that new channels use the same media by default. Channels can associate dependent files with a main file, and deliver dependent files as either viewable or hidden. For example, when distributing an HTML page that includes graphic files (required to display the HTML file correctly, but not needed by the user), a channel could send dependent .jpg files as hidden. So although not separately viewable by the user, the graphic files would populate the HTML page correctly.

Afaria makes it cost-effective to deliver and automatically update important documents. It decreases the time mobile workers have to spend navigating through the LAN, Internet, or intranet for pertinent information and makes it easy for content owners to keep content fresh. In doing so, it reduces the total cost of ownership associated with managing content.

Note: Afaria functionality varies by operating system.

AFARIA FUNCTIONS BY PLATFORM

Functionality described in this whitepaper varies by operating system. Device management capabilities are often limited by the operating system. Afaria supports each OS to the depth that the operating system allows. The chart below details components that are available for each operating system.

Afaria Management	iOS	Android	WinMobile	Windows	Symbian	Win CE	RIM	Palm
Application Management	✓	✓	✓	✓	✓	✓	✗	✓
Strong Password Security	✓	✓	✓	✓	✓	✓	✗	✓
Device Configuration	✓	✓	✓	✓	✓	✗	✓	✓
Asset Tracking	✓	✓	✓	✓	✓	✓	✓	✓
Device Encryption	✓	✓	✓	✓	✓	✗	✗	✓
Software License Tracking	✗	✓	✓	✓	✓	✓	✓	✓
Process Automation	✗	✓	✓	✓	✓	✓	✓	✓
AntiVirus and Firewall	✗	✗	✓	✗	✓	✗	✗	✗
Data Backup	✗	✗	✓	✓	✓	✓	✗	✓
Document Distribution	✗	✗	✓	✓	✗	✓	✗	✓

Sybase, Inc.
Worldwide Headquarters
One Sybase Drive
Dublin, CA 94568-7902
U.S.A
1 800 8 sybase

www.sybase.com

SYBASE®
An SAP® Company